Development of Cryptography Algorithms for Improving the Security of Cloud Based IoT

A Ph.D. Proposal

Submitted to

Swami Ramanand Teerth Marathwade University, Nanded, India

For the degree of

Doctor of philosophy in Computer Science

Under

Faculty of Science and Technology

By

Mohammed Ali Qasem Naji

Under the guidance of

Dr. S. B. Thorat

Research Supervisor

Dept . Computer sciences

01/06/2021

Abstract

IoT and cloud are collaborating to create a data-storage-intensive environment in which security is the most important factor for data protection. Cloud computing services offer highly scalable, portable, and storage computing capabilities on a pay-per-use basis. With the increased demand for specific IoT products. The Internet of Things has altered the way things are done in the computing world. This is why cloud computing and IoT device integration is critical, since the amount of data generated by IoT devices necessitates proper and safe storage as well as a processing system. Even so, security issues remain more pressing because users share a vast range of cloud storage capabilities in a variety of ways on their smartphones. In an environment where unsecured data could jeopardise our well-being, privacy is much more important. As a result, the internet of things in cloud computing must constantly ensure that consumers' protection and privacy concerns are always achieved.

This study investigated topics such as stability and solutions for IoT in cloud computing. IoT introduces new protection and privacy problems that must be considered when designing security strategies. The heterogeneous natures of IoT communications, as well as the imbalance in resource capacities between IoT devices, make it difficult to have the necessary end-to-end encrypted connections. This study investigated topics such as stability and solutions for IoT in cloud computing. IoT introduces new protection and privacy problems that must be considered when designing security strategies. The heterogeneous natures of IoT communications, as well as the imbalance in resource capacities between IoT devices, make it difficult to have the necessary end-to-end encrypted connections. Since certain. As a result, the possible choices of security solutions are limited. The findings highlight the major security issues and risks that still need to be discussed. This study addresses the various security issues confronting IoT in cloud computing, with a focus on consumer privacy which concers security by using the cryptography algorithms.

Cryptography is a valuable security technique (algorithm) that can be described as translating plaintext (original text) into cipher text (mysterious text) and reversing from cipher text (mysterious text) into plaintext (original text). These operations are known as cypher encryption and decryption. These operations are called encryption and decryption by using a cipher. Conventional cryptography has different standard algorithms like the Advanced Encryption Standard (AES) algorithm, and Data Encryption Standard (DES) algorithm. The aim of this research is also to explore and improve critical security strategies for data encryption and decryption in cloud computing for IoT. Furthermore, data security algorithm would be proposed in order to improve iot in cloud computing.

Keywords: Internet of Things, Security, Cloud computing, privacy

Table of Contents

Abstract 2

Table of Contents 3

1. Introduction 4

2. Literature Review 6

3. Motivation: 11

4. Problem statement: 11

5. Objectives 12

6. The proposed model 13

7. Methodology 13

8. Time plan 14

References and Bibliography 15

1. Introduction

In our day and age, Information Systems have provided organizations with more efficient means of data management, collection, and mining at the cost of hardware, software, and Information Technology solutions. Hence, these organizations are striving to find more suitable and cost-efficient means of conducting their IT-sector using better tools and technologies IoT and cloud are collaborating to create a data-storage-intensive environment in which security is the most important concern for data privacy. Cloud computing refers to platforms that offer pay-per-use computing capabilities that are extremely scalable, portable, and storage-intensive [1]. Cloud hosting systems for computation and storage are becoming more common, and many businesses are now transferring data from their in-house network networks to Cloud Storage Providers (CSPs).

With the increased demand for such IoT applications, there will be an increase in the production of software that will face security problems when linking to cloud providers. A modern wave of Internet of Things technologies will be able to offer more advanced services based on increasingly fine-grained data processing in an environment heavily populated with smart things in the future. In recent years, there has been an increase in the number of IoT devices such as advanced building management systems; public monitoring, smart city services, and even participatory sensing that allow users to do their job more effectively [2]. Traditional processing and cloud infrastructure can also face challenges in handling time-varying workloads and large data in IoT applications. Furthermore, the encryption mechanisms are not as strong as they can be, and the third-party auditors charged with managing the data and ensuring its accuracy are also in their early stages of growth. The amount of data gathered on persons by many government agencies is the at a higher rate per year, making it more difficult for people to consider the implications. This kind of data increases the likelihood of privacy problems. Ignorance of these issues may have long-term detrimental consequences, such as non-acceptance of technology, failure of emerging technology due to reputation issues, and costly litigation [3].cloud computing and IoT have spread globally and expanded quickly in recent years[4]. The characteristics they show can be outstanding when combined. They are each really special and important for each other [5]. Researchers scheduled a range of applications concerning Coordination of Cloud and IoT to develop and accumulate data as it gets assistance from cloud storage and computational capability. In this part, then explain the Cloud-IoT (Cloud and IoT) architecture. The layers of knowledge in Fig1 are explained below. The application, network, and sensing layers are interconnected.

A variety of cryptographic methods can be used to deal with the security problem; these methods are not suitable for constrained IoT devices. The IoT devices have limited resources in terms of CPU and

memory, this means they often transmit data only when there is something important was triggered or sensed. As a solution the security issue is offloaded to the fog or the edge nodes within IoT networks, which security and data analysis directly handled by the edge of the network. The algorithm of cryptography provides a high-level security but does not take into account the hardware/software requirements; power consumption (cycles of encryption/decryption), code size, and memory overhead. Since, the traditional cryptographic does not focus on the hardware/software requirements, it is not suitable to work on very low computing power devices. Due to the tremendous sophistication of technology everywhere and the inefficiency of practical applications and complicated mathematical processes in traditional cryptography, which are also expensive in processing and memory space.

Integrating the principle of cryptography on the functional shortcomings of IoT devices is desirable. Using cryptographic algorithms in IoT devices, the data will be secured and integrated before it is published on the back-end networks (cloud server or other). While security based on cryptography is increasingly necessary. However, the security based on the approved encryption algorithms is a big challenge in the hardware/software of IoT due to the large area and consumption of power. In addition, the encryption operations in the Internet of Things must contain robust and effective management for the public key. The strong key management leads to the protection of data integration and security. IoT devices are essentially lightweight, meaning that they should have a little storage capacity. Furthermore, IoT devices are mostly battery-driven; as such, low power consumption is required. Therefore, the symmetric key cryptography algorithms are commonly preferred for the design of IoT devices due to their lower computing capacity, storage space, complexity in comparison to the asymmetric key cryptography algorithms, which take more process and more memory.

Block cypher is a form of secret key cryptography that was developed in the last decade to improve resource-constrained computing devices due to its simplified software and hardware implementation and wider adoption. In comparison to the stream cypher, it necessitates extremely limited hardware resources [4]. Traditional Feistel cyphers, on the other hand, take a long time and use a lot of resources because they require a lot more circular functions than replacement-permutation networks (SPNs).

In this regard, a convergence of the Feistel and SPN systems has been proposed in a single structure. The synthesis framework offers lightweight and compact circular functions with low energy consumption and storage, and it aids in rapid diffusion [11]. In light of all the difficulties and disadvantages of tiny IoT devices, a LW symmetric key cryptographic strategy has been suggested here by improving all the susceptibilities present in existing literature.

Hence, security is the main challenge in IoT devices and the implementation of IoT services depends on protecting this technology against unwanted threats and security attacks (Sharma and Kalra 2018).

Cryptography schemes prepare a fundamental security layer for data and various applications. Recently, with the rise of IoT, we need lightweight and efficient cryptographic schemes (Saha et al. 2019).

To have successful access control on the IoT, several principles and features must be considered (Qiu et al. 2020b). The most important features that should be considered in access control are: confidentiality, data accuracy, and information access levels. Access control method can effectively monitor the access activities of resources, and ensure authorized users to access information resources under legitimate conditions (Li et al. 2019; Tian et al. 2020b). Ensuring data security is a very important factor in building trust on users and using the IoT platform. Users need to make sure that the IoT is secure enough to carry out security activities against threats. Therefore, considering the confidentiality of data means the formation of trust in IoT (Chen et al. 2019).

The aim of this reserch is to develop a new model for protecting sensitive data of IoT in cloud computing the main aim Increasing security with encryption efficient for data transport scheme for the IoT in cloud environment.

2. Literature Review

1. Security Challenges in Internet of Things

Some of the security concerns surrounding the IoT devices in cloud computing include hijacking of IoT devices or ransomware, theft of IoT devices, unauthorized use of the internet, rogue devices, home invasions, and a variety of other potential risks.

- Hijacking and Ransomware

  Smart- Home devices, wearables devices, and audio-video devices that are connected to cloud services can become targets of Ransomware. Malicious malware that gains access to a user's files, encrypts, and blocks the user from accessing their sensitive files. When a hacker attacks an IoT device with ransomware, they can take control of the device and demand money if the victim hopes of seeing their encrypted files unlocked. Fortunately, it is a rare reality as of yet. But, this is a serious challenge in the hacking community and among the hackers themselves [4]. This security concern can put a smart home, healthcare trackers, and wearable technologies at risk. It is a disturbing thing to learn someone's smart house is hacked and locked down or even a smart vehicle that cannot be started until a ransom is paid. If the ransomware threats like some that have gone on in recent times win the battle, this could shut the user out of their devices and potentially lead to a loss of the user's data. The rapid expansion in the Internet of things technologies will cause some security concerns that will be unpredictable [5]. Even so, the bottom line regarding data theft is that most of the information is stored in a highly encrypted

cloud, so it is very unlikely the person will have any worthwhile information to steal. According to one report, some IoT manufacturers do not provide necessary security and software updates [6].

- There are insufficient testing and a lack of updates.

Another security challenge with the Internet of Things (IoT) is that many companies producing IoT devices are not properly chosen and often too disorganized to properly fix security-related software updates. Since consumers usually trust manufacturers who are often confident that they are in control of product safety, it becomes a big problem to the user in case of a security failure [7]. Although there is indeed a rapid growth of the Internet of Things platform, it is also true that a lot of manufacturing companies are swooping into the market without offering the marketing research much consideration. Web sites that offer shorter periods also don't usually offer consistent updates. The reason for these updates is because of the rise in a shortage of devices. As a result, they make the new generation of devices that they ask the users to start using them without proper security measures [8]. If the IoT device has outdated software installed in it, it may be prone to numerous malicious attacks from hackers and other security breaches. There is also another risk of downtime when an IoT device sends its information to the cloud. During an upgrade, some parts of the app might stop functioning while others search for updated components of the app and submit the updated data. Firmware versions that are A49 and B06 have bugs that may lead to a more insecure router, so it is advisable to upgrade the firmware versions as soon as possible [9]. Given the many "internet of things" security risks, proper automatic updates are of paramount importance. The manufacturer of IoT devices has a duty of updating their devices into the latest software as soon as a vulnerability is detected and when a malware attack is discovered.

- Home invasion

The most distressing scenario of the Internet of Things (IoT) security challenges is when users of IoT devices experience home invasions. Smart devices are currently extending into every part of our lives. The fact that many of our homes are connected to the Internet, has given rise to the concept of smart homes. The biggest problem with smart home systems is that, if there is any security loophole, there is a big risk of them broadcasting IP addresses to nearby hackers. The search engine Shodan can help out hackers in finding out the location of the user of the device. In terms of abuse, what can be concluded is that this technology can reach criminal circles and can be sold to the public [10]. As an introduction, the way to prevent that IoT security flaw from occurring is by configuring each device to connect through VPNs, considering the importance of passwords, and securing the login details.

- Financial crime resulting from the Internet of Things.

As the Internet of Things payment companies deploys their internet of things, they should anticipate an increase in future identity theft and other financial crimes A few of these firms have focused on automation and artificial intelligence, while most of them will eventually need to be able to acknowledge the significance of integrating security measures on different company levels. To ensure that fraud detection programs remain more effective, they must continuously monitor their data source for new fraud patterns. All financial firms will experience reservations about the adoption of these new models because they face several issues on compliance and operational aspects [11]. In simple terms, IoT security breaches can take many different shapes, including (but not limited to) attacks of different systems, smart-protocol failures, and IoT device hacks.

- Remote Smart Vehicle Access

The hijack of smart cars is close to a security threat of home invasion. Vulnerable Internet of Things (IoT) devices can lead to vulnerabilities in smart cars, such as remote hijack of the car's access [12]. Compromising the vehicle's functionalities can affect the vehicle's autonomous capabilities to operate like self- driving functionalities and detection of other vehicles. There have been many cases of threats to public safety concerns that have caused injuries. Losing access to the car can also be subject to a tie into remote hacking especially when a hacker locks the car's doors and demands payment for unlocking or enabling the engine many cars and IoT device manufactures are paying close attention to the many security breach issues. However, car manufacturers like BMW and Honda are also paying attention to these security breaches. Microsoft and Ford Motor have come up with an infotainment system that is completely vulnerable and open to these types of attacks [12]. The developers addressed several forms of these attacks, with their preferred solutions one of the simplest of which was a deliberate upgrade to a more secure infrastructure and software package. The future introduction of remote-control cars will pose a major security threat to IoT devices.

- Rogue and fake IoT devices

A significant security challenge is the ability to protect a system from being accessed from any one device. There's a challenge with using the IoT in one's home as it can become bulky if one chooses to install more home devices. Users end up mounting rogue and substandard IoT in secured networks without any network authorizations. These devices replace the original network units and/or integrate into the network to obtain confidential information and data, violating the secure perimeter of the network [12,13]. These smart devices have the potential to be turned into rogue access points, thermostats, video cameras, and other forms of devices to intercept network communications without the knowledge of the user.

- The lack of user knowledge about the internet of things (IoT) security.

There are a large number of people who are still learning the quirks and traits of the Internet of Things (IoT). Most users have now perfected their security issues regarding phishing, malware, and viruses on computers or internet fraud. Before they perform internet banking, they spent some time learning about securing their internet connection and also learning how to safeguard their credit cards online. But, as is has been reported, IoT devices still fail, not only due to the manufacturers' limitations but also due to the users themselves, who didn't take the required measures to protect their devices and networks. The lack of computer awareness is the biggest issue with the Internet of Things because it opens up the possibility of abuse by both users themselves, as well as those who would be connected with their own IoT networks [13]. Social engineering hackers target the human factor because it is the most easily bypassed using the Internet of Things. A serious case of the unprepared human factor is the 2010 attack on a nuclear site in Iran, which was and will always be very tragic. The attackers targeted the IoT tool called a programmable logic controller, which meant that the device only needed only one worker to insert a small flash drive into the controller, thus allowing an attacker to penetrate the system in the internal network and make that network public.

2. Cryptography algorithm for IOT in cloud computing

Current cryptographic models and security schemes are based on widely adopted encryption algorithms, and privacy standards. Confidentiality is ensured in most of the cases with Advanced Encryption Standard (AES). The asymmetric algorithm RSA serves for asymmetric encryption, digital signatures, as well as for key management. SHA standards are used as secure hash functions. Alternatively, Diffie-Hellman (DH) and Elliptic Curve Cryptography (ECC) supplement the privacy schemes, basically in asymmetric cryptography. Actually, the applied suites have been designed for general purpose uses, and their functionality is based on significant processing power, good memory resources, and power availability. Since the applicability of these cryptographic models and security schemes is a little bit unclear, detailed analysis is needed, in order to be ensured, that they can be implemented in the specified resources of IoT [15]. Especially in the case, of minimized capabilities of hand-held and portable devices [6]. In addition, other security services, such as key management, are growing up and have to be applied successfully, in future designs [17].

KP-ABE algorithm is used as an appropriate security mechanism for heterogeneous encryption, and is widely deployed for implementing access control solutions. Touati and Challal (2016) used this algorithm for IoT security through three phases: initialization and key generation, data encryption, data decryption and extraction. Encryption is vital for privacy in healthcare plans. IoT demands an efcient and low-energy cryptographic algorithm, Khader et al. (Khader et al. 2017) used modifed AES algorithm to propose a low-energy cryptographic mechanism for IoT sensors. AES is a common method that uses a 128, or 192, or 256-

bits key for encryption and decryption. A hidden ciphertext policy Attribute-based Encryption (ABE) was proposed in (Belguith et al. 2018) that preserved privacy and had low processing overhead.

Privacy and security issues of IoT users were considered in (Wei and Zhou 2018). One essential problem is access to server to obtain information through mobile phones. To this end, homomorphic encryption and ABE were used. Homomorphic encryption allows for direct encryption of an infnite number of calculations without disclosing the secret keys. Dife–Hellman (DH) encryption is also used for IoT security and privacy. It uses RSA heterogeneous encryption to generate keys between the application and the server, and then uses symmetric AES algorithm to encrypt communications between them by the generated key (Xu et al. 2019a). Dife–Hellman encryption is used to deal with security and privacy challenges in IoT cloud. A fast encryption protocol has proposed in cloud servers (Wu et al. 2018). An AES-based encryption scheme with a 128-bit key for building a secure session between things was proposed with high computational efciency, los costs and proved strong against diferent attacks like service denial, response attack, and physical manipulation attack (Jan et al. 2019).

A proper security algorithm for IoT is adopted in terms of time, memory, and processing. Data are encrypted, decrypted and encrypted once again, yielding a 168-bit key that is long enough for many sensitive data. Thus, Triple-DES is a stronger standard than DES. Results of testing the security algorithms show that AES has a better performance in terms of computational time, memory use and processing. The large key length in AES ensures higher protection levels. However, it has some defcits such as inability to authenticate and encrypt diferent data types including videos, photos, and audio fles. Therefore, we used a combination of the above algorithms. A security scheme based on RSA and ECC for IoT data has proposed that used RSA security blocks to promote security level (Chhabra and Arora 2017). A hybrid and secure algorithm for data storage and transmission in IoT cloud was proposed where the data are encrypted by AES before transmission. AES key is encrypted using RSA system. Moreover, RSA encryption key with authorized users is shared through email (Chandu et al. 2017). IoT are vulnerable to malware attacks such as bufer overfows, denial-of-service, and Trojan horse, worms, viruses and malicious codes. These attacks are modifed by RSA and AES algorithms (Abinaya et al. 2018). TLS protocol was tested by RSA in terms of security measures, scalability, power consumption and data usage. The results were the compared to ECC. Key length in ECC provides a reasonable security level. TLS is mostly applied in transmission layer in wired and mobile networks and is used to provide a secure communication. Its specifc mechanisms help establish data confdentiality, integrity and privacy (Suárez-Albela et al. 2018).

RSA is used to enhance cryptography and privacy processes (Hussain et al. 2017). CP-ABE-based RSA was proposed to guarantee a secure communication between IoT server and devices (Odelu et al. 2017). In

(Xu et al. S. K. Mousavi et al. 1 3 2019b), an access control based on attributes on IoT cloud has used that allows the data owners to effectively manage the validity of data users and block unauthorized users.

3. Motivation:

Internet of Things (IoT) is completely a new technology, in the areas of science, industry, engineering, policy etc. It has attracted the main interest of research and development activities, as well as is a famous subject, of both press and social media. The importance of IoT, is the promising transformation of aspects, for everyday living activities and services. In bibliography, there is not a universal definition for this scientific area. With the term IoT, we refer mainly in operating scenarios of network connections and computers capabilities, which refer to several objects, like sensors, and other items not necessarily considered as computing. The main target behind, is to combine different in philosophy, parts such as computers, networks, monitors, controllers etc, of several technologies, in order to make alternative combined operations a reality. IoT implementations make use of common communications models such as: device to device, device to gateway, device to cloud, back end, data sharing etc. Well known sectors, of all these mentioned before, are Ubiquitous Computing, almost all kinds of Networking, Computing Economics, Cloud and Data Technologies etc [1]. Consumer electronics include new IoT products, which referred basically to the widespread use of Internet, as well as oriented to home automation, energy efficient devices, and others related to smart homes [2]. Personal IoT devices are widely spread for health monitoring, medical networks, healthcare services, and for assisted living persons.

Communication technologies and data exchange in networks is one of the most important matters for researchers. Therefore, when exchanging messages in communication networks, it must be simple and secure. This means that, the use of encryption is compulsory when sending / receiving messages. This is to ensure that the messages arrive without any interference or penetration from another person and the insurance of the integrity of the data. In this context, there is data processing and security by traditional encryption algorithms. These algorithms need large mathematical operations and need large memory and power. This does not make them suitable for encryption on Internet of things devices. However, these devices are widely used at the present time in the Internet of things which use new enhanced encryption for balance between performance and security. In addition, the study and survey provided by HP shows that 70% of these devices are liable to attackers [25]. In this context, the proposed research to provide the required safety and save devices power using less memory.

4. Problem statement:

Privacy and security in IoT, is proven one of the most challenging areas, with a number of published works about them the last years. Although, the aspects of IoT cryptography and security, are not completely defined. Alternative and different definitions have been proposed by both industrial parts and research sectors.

IoT is a constrained network. Its device resources such as (microcontroller/microprocessor's computational capability, energy, and memory) are limited and restricted. Therefore, traditional cryptographic algorithms are not an appropriate solution to work on data security in IoT devices due to its heavy computational, large memory and large number of execution cycle.

In this direction, applied methodologies have to be developed, in order to support heterogeneity and scalability, to keep users anonymity and to take care of personal data protection.

- **Security Problem**

  The following problems must be discussed when designing high-security algorithms for data safety in IoT devices

- **Memory Utilization (RAM)**

  Memory use is a major problem in IoT applications, limiting resources. Memory use is a significant issue in IoT systems due to space constraints. As a result of the huge number of rounds that use complex mathematical operations, standard cryptographic algorithms need a lot of memory, making them unsuitable for IoT use.

- **Execution Cycle (Encryption/Decryption)**

  Microcontrollers in IoT devices are limited. As a result, encryption and decryption time (cycles) for IoT devices is shorter than for conventional encryption algorithms.

- **Power consumption**

IoT devices are powered by battery, so their capacity is limited. The process of processing (decryption/encryption cycles) and transferring data between devices leads to the consumption of devices' power. The execution cycle and energy consumption are related to one another; that is to say, reduced cycle tends to reduce energy consumption, making the algorithms more suitable for IoT devices than traditional encryption algorithms.

5. Objectives

The study seeks to understand the area of Internet of Things (IoT) in cloud computing and cryptography algorithm and to contribute with new security techniques for betterment of the field. In addition, it analyzes the existing schemes in attempts to develop new optimal and secured schemes, leading to the use of simple operations to preserve memory, as well as reducing encryption and decryption cycles to conserve devices power in the Internet of Things. In short, the objectives of the current study can be listed as follows:

- To provide an overview of the emerging Internet of Things (IoT) in cloud computing and related security research work done in this area.
- To present an optimal solution for different security challenges of IoT in cloud in terms of practical use.
- To design and implement cryptographic Algorithm for Securing Data on Internet of Things in cloud.
- To design and implement Energy efficient and low foot print memory cryptographic algorithm for securing data for Io T in cloud environment.

- To give conclusion and recommendation for future work.

6. The proposed model

In this section Development Cryptography Algorithm for Improving the Security Internet of Things in Cloud Computing using the information stated in the previous section is offered. We aim to study the cloud computing security techniques and we will work to new enhanced techniques for security in cloud computing.

Figure 1: The proposed model

7. Methodology

We aim to development cryptography algorithm for improving the security internet of things in cloud computing First, we will study the literature and the real techniques are used for security the security internet of things in cloud computing. This will be according to a study for many previous related works with the security internet of things in cloud computing in every possible field (integrity and confidentiality). Then will suggest which technique of the security which we will work on it , we will suggest the needed standards and circumstances adopt the resulted model in order to have a the security internet of things in cloud computing . The final step will be to develop a sample example for the model and to test it to prove that it is applicable.

8. Time plan

Table 1: Time Schedule

Stage of the dissertation writing process	Number of weeks needed	Start date	End date
STAGE ONE: Reading and research			
a) Seek to identify an original, manageable topic	2	01/05/2021	14/05/2021
b) Reading and research into chosen topic	3	15/05/2021	5/06/2021
STAGE TWO: The detailed plan			
a) Construct a detailed plan of the dissertation	3	06/06/2021	26/06/2021
STAGE THREE: Initial writing			
a) Draft the various sections of the dissertation	12	27/06/2021	18/09/2021
b) Undertake additional research where necessary	6	19/09/2021	08/11/2021
STAGE FOUR: The first draft			
a) Compile and collate sections into first draft of dissertation	30	09/11/2021	05/08/2022
b) check the flow of the dissertation	6	06/08/2022	17/09/2022
c) Check the length of the dissertation	3	18/09/2022	15/10/2022
d) Undertake any additional editing and research	3	16/10/2022	12/11/2022
STAGE FIVE: Final draft			
a) Check for errors	25	13/11/2022	07/05/2023
b) Prepare for submission	6	08/05/2023	19/05/2023
c) Final proof-read (by a friend or yourself) and final editing	12	20/05/2023	12/08/2023
d) Compile bibliography	4	13/08/2023	11/09/2023
e) Get the dissertation bound	5	12/09/2023	16/10/2023
f) Submit your dissertation	15	17/10/2023	02/02/2024

References and Bibliography

[1]. C. Tomer. "Cloud computing and virtual machines in: options and resources." *Digital Library Perspectives* 33.1 (2017).

[2]. Abinaya E, Aishwarva K, Lordwin CPM, Kamatchi G, Malarvizhi I (2018) A performance aware security framework to avoid software attacks on Internet of Things (IoT) based patient monitoring system. Int Conf Curr Trends Towards Converg Technol (ICCTCT). https://doi.org/10.1109/ICCTCT.2018.8550955

[3]. Agale RR, Gaikwad DP (2017) Automated irrigation and crop security system in agriculture using Internet of Things. Int Conf Comput Commun Control Autom (ICCUBEA). https://doi.org/10.1109/ICCUBEA.2017.8463726

[4]. Alaba FA, Othman M, Hashem IAT, Alotaibi F (2017) Internet of Things security: A survey. J Netw Comput Appl 88:10–28 Azari L, Ghafari A (2015) Proposing a novel method based on network-coding for optimizing error recovery in wireless sensor networks. Indian J Sci Technol 8:859–867

[5]. Babayiğit B, Büyükpatpat B (2019) Design and implementation of IoT-based irrigation system. Int Conf Comput Sci Eng (UBMK). https://doi.org/10.1109/UBMK.2019.8907066

[6]. Belguith S, Kaaniche N, Laurent M, Jemai A, Attia R (2018) PHOABE: Securely outsourcing multiauthority attribute based encryption with policy hidden for cloud assisted IoT. Comput Netw 133:141–156

[7]. Burton L, Dave N, Fernandez R, Jayachandran K, Bhansali S (2018) Smart gardening IoT soil sheets for real-time nutrient analysis. J Electrochem Soc 165:B3157

[8]. Chandu Y, Kumar KSR, Prabhukhanolkar NV, Anish AN, Rawal S (2017) Design and implementation of hybrid encryption for security of IOT data. Int Conf On Smart Technol Smart Nation (SmartTechCon). https://doi.org/10.1109/SmartTechCon.2017.8358562

[9]. Chen J, Tian Z, Cui X, Yin L, Wang X (2019) Trust architecture and reputation evaluation for internet of things. Ambient Intell Humaniz Comput 10:3099–3107. https://doi.org/10.1007/s1265 2-018-0887-z

[10]. Chhabra A, Arora S (2017) An elliptic curve cryptography based encryption scheme for securing the cloud against eavesdropping attacks. Int Conf Collab Internet Comput (CIC). https://doi.org/10.1109/CIC.2017.00040

[11]. Ghafari A (2014) Designing a wireless sensor network for ocean status notifcation system. Indian J Sci Technol 7:809

[12]. Ghafari A, Rahmani A (2008) Fault tolerant model for data dissemination in wireless sensor networks. In: 2008 International Symposium on Information Technology, IEEE, pp 1–8.

[13]. Ghafari A, Takanloo VA (2011) QoS-based routing protocol with load balancing for wireless multimedia sensor networks using genetic algorithm. World Appl Sci J 15:1659–1666

[14]. Gilbert H, Handschuh H (2004) Security analysis of SHA-256 and Sisters. In: Matsui M, Zuccherato RJ (eds) Selected areas in cryptography, Berlin, Heidelberg. Springer, Berlin, pp 175–193

[15]. Gulati A, Thakur S (2018) Smart irrigation using Internet of Things. Int Conf Cloud Comput Data Sci Eng (Conflu). https://doi. org/10.1109/CONFLUENCE.2018.8442928

[16]. Hamidi H (2019) An approach to develop the smart health using Internet of Things and authentication based on biometric technology. Future Gener Comput Syst 91:434–449. https://doi.org/10.1016/j. future.2018.09.024

[17]. Han Q, Zhang Y, Li H (2018) Efcient and robust attribute-based encryption supporting access policy hiding in Internet of Things. Future Gener Comput Syst 83:269–277. https://doi.org/10.1016/j. future.2018.01.019

[18]. Hendrawan INR, Yulyantari LP, Pradiptha GA, Starriawan PB (2019) Fuzzy based internet of things irrigation system. Int Conf Cybern Intell System (ICORIS). https://doi.org/10.1109/ICORI S.2019.8874900

[19]. Hu Z (2011) A method for the signature of things. In: International Conference on Intelligence Science and Information Engineering, pp. 366–369.

[20]. Hussain I, Negi MC, Pandey N (2017) A secure IoT-based power plant control using RSA and DES encryption techniques in data link layer. Int Conf Infocom Technol Unmanned Syst. https://doi. org/10.1109/ICTUS.2017.8286054

[21]. Jan MA, Khan F, Alam M, Usman M (2019) A payload-based mutual authentication scheme for Internet of Things. Future Gener Comput Syst 92

The Researcher/Student **The Research Guide**

Mohammed Ali Qasem Naji **Dr. S. B. Thorat**